IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Gregorio RODRIGUEZ, et al. Atty. Ref.: 4020-3

Serial No. 10/510,498 TC/A.U.: 2617

Filed: October 7, 2004 Examiner: Sayed T. ZEWARI

Confirmation No.: 1556

For: SYSTEM, APPARATUS AND METHOD FOR SIM-BASED AUTHENTICATION AND ENCRYPTION IN WIRELESS LOCAL AREA NETWORK ACCESS

* *

September 11, 2008

MAIL STOP AF
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

The rejection of claims 1-5, 7-13, 15-22, and 24-25 is clearly erroneous because US Publication 2002/0012433 A1 to Haverinen et al. (hereinafter "Haverinen") fails to teach or suggest all claimed features. The present disclosure generally describes a telecommunication system for allowing a SIM-based authentication to users of a wireless local area network (WLAN) who are subscribers of a public land mobile network (PLMN). Fig. 1 illustrates a general scenario where subscribers of a PLMN (such as GSM/GPRS/UMTS), and other local non-mobile users, access a WLAN. *See paragraph [0046] of the disclosure as originally submitted.*

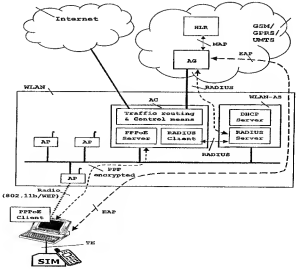


FIG.-1-

In an embodiment, the Terminal Equipment (TE), which is an example of a wireless terminal, is equipped with the necessary hardware and software to interface the user's SIM card and to send and receive the required signaling information according to the Authentication and Key Agreement (AKA) protocol as well as to implement a Point-to-Point Protocol over Ethernet (PPPoE) protocol. *See paragraph [0047].* Fig. 4 illustrates an example sequence of actions carried out from the TE to the mobile network and throughout the WLAN entities to perform the SIM-based authentication.

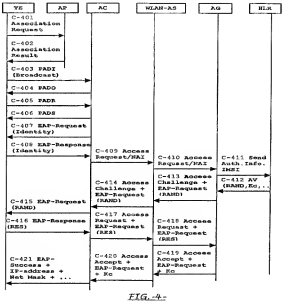


FIG. 4

As shown, the TE initially accesses the WLAN through an Access Point (AP). The Access Controller (AC), which is interposed between the AP and the PLMN, is then discovered. Afterwards, a challenge-response authentication procedure is carried out between the PLMN and the TE through the AC. The IP connectivity is provided after the challenge-response authentication takes place.

Method claim 1 recites, in part "carrying out a challenge-response authentication procedure between the wireless terminal and the public land mobile network through the Access Controller, the wireless terminal provided with a SIM card and adapted for reading data thereof; the method characterized in that the challenge-response authentication submissions in step (c) takes place before having provided an IP connectivity to the user" and "offering the IP connectivity to the user at the wireless terminal, by sending an assigned IP address." As recited, the wireless terminal is first authenticated, and then the IP connectivity is provided.

The quoted steps are missing from Haverinen. The June 7, 2008 Office Action ("Office Action") relies upon Figs. 7 and 8 of Haverinen and corresponding explanations on paragraphs [0242]-[0258] for these features of claim 1. Fig. 7 merely shows an architecture of a mobile

communication system, and Fig. 8 illustrates functional blocks of the system of Fig. 7. *See paragraphs [0241], [0248] and [0256].* Neither illustrate the signaling steps. However, Fig. 9 of Haverinen, reproduced below, does illustrate the major signaling steps of the system of Figs. 7 and 8. *See paragraph [0263].*

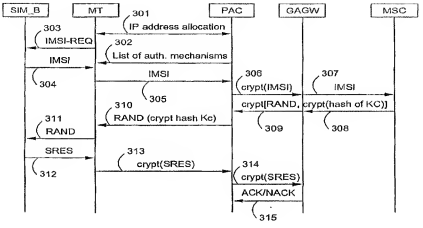


Fig. 9

In step 301, which is the very first step, the mobile terminal (MT) communicates with the public access controller (PAC) to obtain an IP address from a DHCP server. *See paragraph [0265].* Subsequent to step 301, the authentication procedure is performed to authenticate the MT to the mobile switching center (MSC) of a mobile network. *See paragraphs [0265]-[0279].* So in Haverinen, the IP address is allocated to the mobile terminal prior to authenticating the mobile terminal with the underlying mobile network. This is in clear contrast to independent claim 1 in which the IP connectivity is provided after authenticating the wireless terminal.

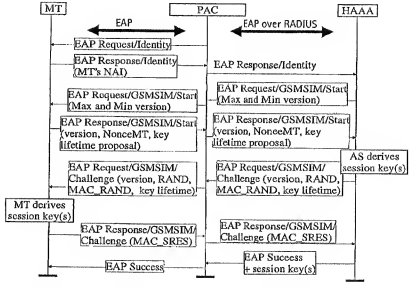
Despite this demonstration, the Office Action declares that Haverinen does not disclose allocating IP address prior to authentication. *See e.g., Office Action, page 2.* The Office Action also alleges it is common knowledge that authentication always takes place before any device is connected to a network and refers to Svensson (US Publication 2003/0120920), paragraphs [0025] and [0026] for support.

There are clear errors with this allegation. First, Svensson is not relied upon in the rejection. If Svensson is to be relied upon, the rejection should have been properly be given under §103 and the combinability of Svensson with Haverinen should have been demonstrated. Second, even assuming arguendo that Svensson is combinable with Haverinen, Svensson does not correct the deficiencies of Haverinen. Svensson merely discloses authenticating a non-provisioned device 18 to a network using a provisioned device 12. The non-provisioned device 18 communicates with a WLAN 20 across an

IEEE 802.11(b) interface and communicates with the provisioned device 12 across a BLUETOOTH interface. Svensson is silent regarding whether IP addresses are allocated after the authentication. *See e.g., Fig. 2 of Svensson.*

Claim 1 also recites that the challenge-response authentication submission are carried "on top of a Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller and on an authentication protocol residing at an application layer between the public land mobile network and the Access Controller." This feature is also missing from Haverinen.

The Office Action alleges that Haverinen discloses this feature at paragraph [0343]. Paragraph **[0343]** should be understood in the context of paragraphs [0342]-[0346] with due regard to Fig. 16, reproduced below, in which Haverinen teaches an authentication procedure being carried out with an Extensible Authentication Protocol (EAP), which is a type of Point-to-Point Protocol (PPP), so that authentication data are exchanged between the MT and the public land mobile network (HAAA) via the PAC.



Here, the PAC does not know details of the authentication. The EAP protocol is used for exchanging authentication data between the MT and the PAC, and an EAP over RADIUS protocol is used for exchanging authentication data between the PAC and the public land mobile network (HAAA).

In contrast to Haverinen, in claim 1, the authentication submissions are carried out on top of the Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller, and on an authentication protocol residing at application layer between the public land mobile network and the Access Controller. PPPoE is not EAP. Further, there is no suggestion in Haverinen

that a challenge-response authentication is carried on top of the PPPoE. In Fig. 16 and corresponding paragraphs, there is no mention of IP connectivity occurring either before or after authentication.

Independent claim 15 recites, in part "wherein the Access Controller is configured to send an assigned IP address and other network configuration parameters to the wireless terminal to provide IP connectivity after the challenge-response authentication procedure is successfully carried out between the wireless terminal and the public land mobile network in the telecommunication system" and independent claim 24 recites, in part "wherein the wireless terminal is configured to receive an IP address after successfully carrying out the challenge-response authentication procedure, the IP address being usable to gain IP connectivity." For reasons explained for claim 1, the quoted features of claims 15 and 24 are missing from Haverinen.

Thus, the rejections of independent claims 1, 15, and 24 are clearly erroneous. Claims 2-5, 7-13, 16-22, and 25 depend from independent claims 1 and 15. Due to at least the dependencies thereon, rejections of these dependent claims are also clearly erroneous. The rejections of claims 6, 14, and 23 are clearly erroneous since none of the cited secondary references US Patent 7,043,633 to Fink et al. and US Patent 6,854,014 to Amin et al. correct at least the above-noted deficiencies of Haverinen.

CONCLUSION

As shown by the above analysis, the claimed subject matter not anticipated or rendered obvious. The prior art rejection should be withdrawn, and the pending claims allowed.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
Hyung N. Sohn
Reg. No. 44,346

HNS/edg
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100